REMARKS

In the Office Action, dated October 31, 2005, the Examiner states that Claims 1-4 and 14-23 are pending and Claims 1-4 and 14-23 are rejected. By the present Amendment, Applicant amends the claims.

In the Office Action, Claims 4, 15 and 16 are objected to for various informalities. Claim 4 has been amended to correct the typo. Claim 15 has been amended to recite "A device". Claim 16 has been cancelled and reintroduced as new Claim 24, which depends from Claim 17.

In the Office Action, Claims 1-4 and 14-21 are rejected under 35 U.S.C. §103(a) as being unpatentable over Mapson (WO 98/32260) in view of Schneier et al. (US 5,956,404). The Applicant respectfully disagrees with and traverses this rejection.

Claim 1 of the present application recites, among other features, *A method for securely encoding and transmitting a message...said message being associated with a particular one of a plurality of applications running on the originating device, the method comprising the steps of: (a) determining a device identifier for the originating device, and an application identifier for each of the plurality of applications...(d) generating a message value...using the device identifier, a particular application identifier and an application value...(e) combining the message value with said secret value...to establish a corresponding secret message value;...(g) combining the device identifier the particular application identifier the application value and the secure message block to form a secure message for transmission, said secure message being decodable, dependent upon the device identifier, the particular application identifier and the application value...*

The *secure message for transmission* is the "transmission data block 606". This can be clearly seen by referring to 606 both in FIG. 6 (which, together with FIG. 5 relates to formation of the message for transmission) and in FIG. 8 (which, together with FIG. 9 relates to use of the received message to recover the message data 600). It is apparent that the *secure message for transmission* includes, in unencrypted form, the (i) *device identifier* (ii) *the particular application identifier* (iii) *the application value, and* (iv) *the secure message block.* The *secure message* can

be decoded *dependent upon the device identifier, the particular application identifier and the application value.*

It is also noted, from *(a)* and *(d)* above that the *device identifier* is used to generate the *message value* which is subsequently used to *establish a corresponding secret message value*. Accordingly, the *device identifier* in Claim 1 is used in the encoding process.

Therefore, the *secure message* which is transmitted contains features (i) – (iv), and features (i)-(iii) are used at the receiver for decoding the *secure message* from (iv). Furthermore, the *device identifier* is used in the encoding process.

The *application identifier* in Claim 1 has significant utility to a user. This is illustrated in the description at page 12 line 7 to page 13 line 3. This depicts how the disclosed secure communication arrangement can be used in a practical context in which a user wishes to communicate securely using a number of applications such as remote access v1.01, application no. 1098756, ABC savings account Cash Management v2.9 and so on.

Mapson discloses in FIG. 4 an assembled purchase transaction (see page 5 lines 31-32), this being a message for transmission, which comprises a plain text (unencrypted) data block including (a) an unencrypted Device ID (see page 2 line 8 which refers to the unencrypted first identifier, this being associated with the transmitting means as stated at page 2 line 4); and (b) an unencrypted random number R1 (see page 2 line 25). The random number is used to generate a transaction-specific unique encryption key for each transaction (page 2 lines 22-24), and the receiving means uses the received random number to decrypt the message (page 2 lines 27-28).

Although Mapson hints at the suitability of the invention for different applications (e.g., page 1 lines 6-8), Mapson neither discloses nor suggests (A) *a plurality of applications running on the originating device or* (B) *determining...an application identifier for each of the plurality of applications, or* (C) *combining the device identifier the particular application identifier the application value and the secure message block to form a secure message for transmission* (emphasis added).

Mapson uses only the encrypted Device ID and the random number R1 to decrypt the encrypted certificate data shown in FIG. 3 (page 2 lines 27-28) and uses

a transaction number T1 (page 5 lines 20-21) also referred to as a second identifier (page 2 lines 5-6) to detect if the transaction is valid (e.g., page 2 lines 10-14).

Furthermore, Mapson does not disclose using the *device identifier* (i.e., the first unique identifier at page 2 line 4) in the encoding process, and in fact uses only a secret value and a random value in the encoding process (Figs. 2 and 5, and page 8 lines 20-26).

There is no disclosure or suggestion in Mapson that the *device identifier* be used in the encoding process, **OR** that multiple applications can run on the disclosed arrangements, **OR** that identifiers for these multiple applications be defined and used in the *secure message for transmission* **OR** that *the particular application identifier be used in decoding the received message.*

Schneier is directed to an encryption scheme that has a strong audit trail while not wasting valuable message space. A strong audit trail may include device token ID bits (column 4 line 5), key ID bits (column 4 line 6) and so on. However, the audit trail enables the user to trace back to see what has happened (column 3 lines 27-30) and does not relate to running multiple applications on a platform is no disclosure or suggestion in Schneier that the *device identifier* be used in the encoding process **OR** that multiple applications can run on the disclosed arrangements, **OR** that identifiers for these multiple applications be defined and used in the *secure message for transmission* **OR** that *the particular application identifier* be used in decoding the received message.

Establishment of a *prima facie* case of obviousness requires that the prior art references when combined must teach or suggest all the claim limitations. Even presupposing that Mapson and Schneier are combined, and having regard to Claim 1, neither citation makes mention of or suggests (A) *a plurality of applications running on the originating device,* or (B) *determining...an application identifier for each of the plurality of applications,* or (C) *combining the device identifier the particular application identifier the application value and the secure message block to form a secure message for transmission* or (D) using the *device identifier* in the encoding process. Accordingly, even presupposing that Mapson is combined with Schneier, it is submitted for at least the reasons noted, that Claim 1 is patentable over Mapson and Schneier whether the references are considered alone or in combination.

The other independent claims recite the same or equivalent features to those of Claim 1, and accordingly it is submitted for at least the reasons noted, that those claims, and the claims dependent thereto, are patentable over Mapson and Schneier whether the references are considered alone or in combination.

In light of the foregoing response, all the outstanding objections and rejections are considered overcome. Applicant respectfully submits that this application should now be in condition for allowance and respectfully requests favorable consideration.

Respectfully submitted,

January 31, 2006
Date

Attorney for Applicant
Brian W. Hameder
c/o Ladas & Parry LLP
224 South Michigan Avenue
Chicago, Illinois 60604
(312) 427-1300
Reg. No. 45613